United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at
10 a.m. EST
Wednesday,
March 13, 2002

VA INFORMATION TECHNOLOGY

Progress Made, but Continued Management Attention Is Key to Achieving Results

Statement of David L. McClure
Director, Information Technology Management Issues

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

20020314 107

GAO
Accountability * Integrity * Reliability

GAO-02-369T

Mr. Chairman and members of the subcommittee:

We are pleased to participate in today's continuing dialogue on the Department of Veterans Affairs' (VA) information technology (IT) program. IT is key to helping VA effectively serve our nation's veterans, and over the years, the department has expended substantial resources (more than $6 billion over the last 6 years) in support of its IT needs. As you know, however, VA has encountered persistent challenges in managing IT to produce results and improve performance.

When we testified before the subcommittee last April, a new secretary of veterans affairs had just been confirmed and an executive-level security officer had been hired.[1] To his credit, the secretary readily seized upon the seriousness of the issues that have been raised concerning VA's IT program, and committed to reforming how the department uses information technology. Since then, VA has also hired a department-level chief information officer (CIO) to lead its IT program. We view this executive leadership as a positive and significant step forward in the department's attempt to achieve better returns on its IT investments. However, VA's IT investment and management challenges are significant, and its ability to resolve them with the right combination of people, processes, and technology that are focused on achieving solid results will take sustained time, effort, and commitment.

At your request, we have been reviewing VA's continuing actions to address critical weaknesses in its overall IT program. Today, we will share with you the results of our work to date regarding VA's actions since last April to

- develop an enterprise architecture;
- improve information security;
- implement the Veterans Benefits Administration's veterans service network project that is intended to replace its existing compensation and pension payment system with a new system;
- extend the usage of, and standardize data collection for, the Veterans Health Administration's decision support system, being used to facilitate managers' and clinicians' analyses of patient care and cost of providing health care services; and
- implement jointly with the Department of Defense and Indian Health Service, the government computer-based patient record initiative,

[1]U.S. General Accounting Office, *VA Information Technology: Important Initiatives Begun, Yet Serious Vulnerabilities Persist,* GAO-01-550T (Washington, D.C.: April 4, 2001).

which was intended to allow physicians and users to access data in each others' health information systems.

In doing this work, we analyzed relevant documentation and interviewed key agency officials to identify and assess VA's progress in implementing specific actions since April 2001 related to developing an enterprise architecture, improving information security, developing the Veterans Benefits Administration's veterans service network compensation and pension replacement system, extending usage of the Veterans Health Administration's decision support system, and advancing data sharing via the government computer-based patient record project. We performed our work in accordance with generally accepted government auditing standards, from June 2001 through March 2002.

Results in Brief

Over the past year, VA has clearly benefited from the commitment of the secretary and other top leaders to addressing critical weaknesses in the department's management of information technology. As a result of their leadership, VA has made important strides in raising corporate awareness of the department's needs and in articulating and acting upon a vision for achieving improvements in key areas of IT performance. Despite this progress, however, many aspects of VA's IT environment remain troublesome, and our message today reflects concerns that we have long viewed as significant impediments to the department's effective use of IT to achieve optimal agency performance. As such, VA has more work to accomplish before it can point to real improvement in overall program performance and be assured that it has a stable, reliable, and modernized systems environment to effectively support critical agency decisionmaking and operations.

In an area of growing importance, VA has taken key steps in laying the groundwork for an integrated, departmentwide enterprise architecture—a blueprint for evolving its information systems and developing new systems that optimize their mission value. Crucial executive support has been established and the department has put in place a strategy to define products and processes that are critical to its development. VA is also currently recruiting a chief architect to assist in implementing and managing the enterprise architecture. Significant work, nonetheless, is still required before the department will have a functioning enterprise architecture in place for acquiring and utilizing information systems across VA in a cost-effective and efficient manner. VA's success in developing, implementing, and using a complete and enforceable enterprise architecture hinges upon continued attention to putting in place a sound program management structure—including a permanent chief architect and an established program office—to facilitate, manage, and advance this effort and to be held accountable for its success. In addition, VA must

continue to take steps to identify and collect crucial information describing essential business functions, information flows, strategic plans, and requirements, and produce a well-thought-out sequencing plan that considers management and organizational changes and business goals and operations. Success also hinges on having proactive management focused on ensuring that investment management and systems development and acquisition are closely linked with the enterprise architecture processes. This integration must be done in a manner that best suits the agency's particular organization, culture, and internal management practices.

Information security management is another area in which VA has taken important steps to strengthen its department-level program, including mandating information security performance standards and, thus, greater management accountability for senior executives. It has also updated security policies, procedures, and standards to guide the implementation of critical security measures. However, VA continues to report pervasive and serious information security weaknesses. Thus far, its actions toward establishing a comprehensive computer security management program have not been sufficient to ensure that the department can protect its computer systems, networks, and sensitive veterans health care and benefits data from unnecessary exposure to vulnerabilities and risks. Moreover, VA's current organizational structure does not ensure that the cyber security officer can effectively oversee and enforce compliance with security policies and procedures that are being implemented throughout the department.

Beyond these two key areas of IT management concern, VA and its administrations also have continued to pursue several critical information systems investments that have consumed substantial time and resources, with mixed success. For example, after about 16 years and at least $335 million spent on modernization, the Veterans Benefits Administration (VBA) is still far from a modernized system to replace its aging benefits delivery network, needed to more effectively support its compensation and pension and other vital benefits payment processes. VBA has not adequately addressed several longstanding concerns related to project management, requirements development, and testing—all of which raise uncertainty about whether the ongoing veterans service network (VETSNET) project will deliver a cost-effective solution with measurable and specific program-related benefits.

Conversely, the Veterans Health Administration's (VHA) managers and clinicians have made good progress in expanding their use of the decision support system (DSS) to facilitate clinical and financial decisionmaking. The use of DSS data for the fiscal year 2002 resource allocation process and a requirement that veteran integrated service network directors better account for their use of this system have both raised awareness of and promoted its utility among VHA facilities. Moreover, VHA has begun steps to further improve the accuracy and timeliness of DSS data. As VHA-wide

usage of DSS progresses, sustained top management attention will be crucial to ensuring the continued success of this system.

Lastly, VA has achieved limited progress in its joint efforts with the Department of Defense and Indian Health Service to create an interface for sharing data in their health information systems, as part of the government computer-based patient record initiative. Strategies for implementing the project continue to be revised, its scope has been substantially narrowed, and it continues to operate without clear lines of authority or comprehensive, coordinated plans. Consequently, the future success of this project remains uncertain, raising questions as to whether it will ever fully achieve its original objective of allowing health care professionals to share clinical information via a comprehensive, lifelong medical record.

Promising Beginning, but VA Remains Far from Implementing an Enterprise Architecture

One of VA's most essential yet challenging undertakings has been developing and implementing an enterprise architecture to guide the department's IT efforts. An enterprise architecture—a blueprint for systematically and completely defining an organization's current (baseline) operational and technology environment and a roadmap toward the desired (target) state—is an essential tool for effectively and efficiently engineering business processes and for implementing their supporting systems and helping them evolve. Office of Management and Budget (OMB) guidelines[2] require VA and other federal agencies to develop and implement enterprise architectures to provide a framework for evolving or maintaining existing and planned IT. Guidance issued last year by the Federal CIO Council[3] in collaboration with us further emphasizes the importance of enterprise architectures in evolving information systems, developing new systems, and inserting new technologies that optimize an organization's mission value.

As this subcommittee is well aware, VA has been attempting to develop an enterprise architecture for several years, but without much overall success. Our prior reports and testimony[4] have documented how VA's previous attempts have fallen short of their intended purpose and did not reflect an approach that would result in an integrated, departmentwide

[2]OMB, *Management of Federal Information Resources*, Circular A-130 (Washington, D.C.: November 30, 2000).

[3]Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture, Version 1.0* (Washington, D.C., February 2001).

[4]U.S. General Accounting Office, *VA Information Technology: Improvements Needed to Implement Legislative Reforms*, GAO/AIMD-98-154 (Washington, D.C., July 7, 1998); U.S. General Accounting Office, *Information Technology: Update on VA Actions to Implement Critical Reforms*, GAO/T-AIMD-00-74 (Washington, D.C., May 11, 2000); U.S. General Accounting Office, *VA Information Technology: Progress Continues Although Vulnerabilities Remain*, GAO/T-AIMD-00-321 (Washington, D.C., September 21, 2000); GAO-01-550T.

blueprint. For example, VA's earlier strategy had called for each of its administrations—VBA, VHA, and the National Cemetery Administration—to develop its own logical architecture, which likely would not have resulted in the department's having an integrated architecture, but rather, at least three separate, unrelated architectures. In addition, VA's common business lines had not been adequately involved in prior attempts to develop an architecture. In July 1998 and August 2000, respectively, we recommended that VA take actions to develop a detailed implementation plan with milestones for completing an integrated, departmentwide architecture, and that it include VA business owners in its architecture development. After assuming office last year, VA's secretary vowed to take action to address the inadequacies in the department's approach.

VA Has Taken Important Steps Toward Developing an Enterprise Architecture, But Much Work Remains

Over the past year, VA has made progress in taking specific actions to lay the groundwork for its enterprise architecture. Its most recent set of activities closely adhere to the Federal CIO Council's suggested guidance on managing the enterprise architecture program.

By effectively implementing an enterprise architecture, VA stands to realize a number of important and tangible benefits. For example, an enterprise architecture can

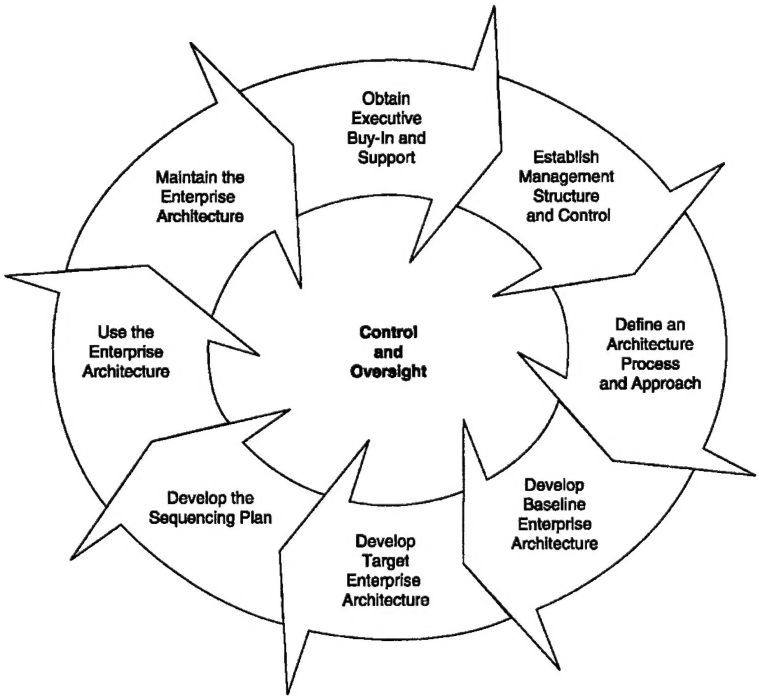
- capture facts about the department's mission, functions, and business foundation in an understandable manner to promote better planning and decisionmaking;
- improve communication among the department's business organizations and IT organizations through a standardized vocabulary; and
- provide architectural views that help communicate the complexity of VA's large systems and facilitate management of its extensive, complex environments.

Overall, effective implementation of an enterprise architecture can facilitate VA's IT management by serving to inform, guide, and constrain the decisions being made for the department, and subsequently decreasing the risk of buying and building systems that are duplicative, incompatible, and unnecessarily costly to maintain and interface.

As depicted in figure 1, developing, implementing, and maintaining an enterprise architecture is a dynamic, iterative process of changing the enterprise over time by incorporating new business processes, new technology, and new capabilities. Depending on the size of the agency's operations and the complexity of its environment, enterprise architecture development and implementation requires sustained attention to process

management and agency action over an extended period of time. Moreover, once implemented, the enterprise architecture requires regular upkeep and maintenance to ensure that it is kept current and accurate. Periodic reassessments are necessary to ensure that the enterprise architecture remains aligned with the department's strategic mission and priorities, changing business practices, funding profiles, and technology innovation.

Figure 1: The Enterprise Architecture Process



Source: *A Practical Guide to Federal Enterprise Architecture*, Version 1.0, 2001

A prerequisite to development of the enterprise architecture is sustained sponsorship and strong commitment achieved through buy-in of the agency head, leadership of the CIO, and early designation of a chief architect. Further, the establishment of an architectural team is necessary to define an agency-specific architectural approach and process. The cycle for completing an enterprise architecture highlights the need for constant monitoring and oversight of architectural activities and progress, and for architecture development teams to work closely with agency business line executives to produce a description of the agency's operations, a vision of the future, and an investment and technology strategy for accomplishing defined business goals. The architecture is maintained through continuous

modification to reflect the agency's current baseline and target business practices, organizational goals, vision, technology, and infrastructure.

In initiating its enterprise architecture process, VA has applied key principles of the Federal CIO Council's guidance and has put in place some core elements of the council's enterprise architecture framework. For example, in the area of executive commitment, the department has obtained crucial buy-in and support from the secretary, department-level CIO, and other senior executives and business teams; this is essential to raising awareness of and leveraging participation in developing the architecture. As evidence of his commitment, last April the secretary established a team made up of VA senior management business line and information technology professionals to develop an enterprise architecture strategy. The team met on weekends over the course of about 60 days and, in August 2001, issued an executive enterprise architecture strategy that articulates the department's policy and principles governing the development, implementation, and maintenance of VA's enterprise architecture.

VA is in the process of establishing committees to manage, control, and monitor activities and progress in fully developing and implementing its enterprise architecture. For example, VA's information technology board has begun functioning as the department's enterprise architecture executive steering committee, with responsibility for directing, overseeing, and approving core elements and actions of the enterprise architecture program. As part of VA's actions to develop and advance its enterprise architecture, it has also chartered an enterprise architecture council—which when activated—is expected to assist in developing project priorities and performing management reviews and evaluations of IT project proposals. In addition, VA is in the process of establishing an enterprise architecture program management office and, over the last 8 months, has been recruiting a permanent chief architect to provide overall leadership and guidance for the enterprise architecture program. These management entities are essential for ensuring that the department's IT investments are aligned with the enterprise architecture and optimize the interdependencies and interrelationships among business operations and the underlying IT that supports them.

Further, as part of its enterprise architecture strategy, VA has chosen a highly recognized enterprise architecture framework that will be used to organize the structure of the architecture.[5] To facilitate its selection of a framework, VA consulted with experts from the private sector and

[5]Among the experts that VA consulted was John Zachman, author of "A Framework for Information Systems Architecture," referred to as the Zachman framework (*IBM Systems Journal*, vol. 26(3), 1987). This framework provides a common context for understanding a complex structure and enables communication among those involved in developing or changing the structure.

borrowed lessons learned from officials involved in architecture development at other federal agencies.

VA has begun defining its current architecture, an important step for ensuring that future progress can be measured against such a baseline, and is also developing its future (target) telecommunications architecture. In addition, to assist in the management of new IT initiatives, VA is considering using a system that it has designed to link the management of its enterprise architecture program to the department's capital planning and project management. It is also considering using a Web-based tool that it has designed to collect data on business rules, requirements, and processes that will be integrated into the enterprise architecture management process.

While VA has taken several important steps forward, it is important to note that the department has many more critical work steps ahead in implementing and managing its enterprise architecture. Using the Federal CIO Council's enterprise architecture guide as a basis for analysis, table 1 illustrates some key steps that have been accomplished, along with examples of the many critical actions VA must still address to implement and sustain its enterprise architecture program. Accomplishing these remaining steps will require continued and substantial time, effort, and commitment.

Table 1: VA's Progress in Developing, Implementing, and Using an Enterprise Architecture

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	Examples of key actions yet to be performed
Obtain executive buy-in and support			
Ensure agency head buy-in and support	✓		
Issue executive enterprise architecture policy	✓		
Obtain support from senior executive and business units	✓		
Establish management structure and control			
Establish technical review committee		VA's enterprise architecture council is expected to perform this function. Council has been chartered; first meeting expected March 2002	
Establish capital investment council		The capital investment review function is part of EA governance in VA's EA strategy The secretary has approved a proposal to integrate VA's EA, capital planning, investment, and project management functions	Define and set policies/procedures for new integrated process Publish the secretary's decision memorandum
Establish EA executive steering committee	✓		
Appoint chief architect		VA has an acting chief architect and is recruiting a permanent one	Hire a chief architect with requisite core competencies
Establish EA program management office		VA is in the process of establishing this office.	Fully staff the EA program management office with experienced architects to manage, control, and monitor development of the EA
Appoint key personnel for risk management, configuration management and quality assurance (QA)		VA plans to staff the positions of EA risk manager and configuration manager April/May 2002 VA's information technology board will perform QA	Ensure adequate staffing occurs and functions are performed Establish an independent, objective entity to perform QA
Establish enterprise architecture core team	✓		

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	Examples of key actions yet to be performed
Develop EA marketing strategy and communications plan		VA has drafted an EA marketing plan	Finalize the marketing plan to include ongoing marketing and communications of VA's EA effort
Develop EA program management plan		VA is drafting the plan; its expected completion date is July 1, 2002	Finalize a plan that will delineate actions to develop, use, and maintain the EA, including management control and oversight
Initiate development of enterprise architecture		VA is developing baseline products, and establishing EA development and management practices.	Complete the EA program management plan to guide VA's EA efforts in developing processes and management practices, training participants, building baseline and target EA products, creating sequencing plan, and populating EA repository[b]
Define architecture process and approach			
Define intended use of architecture	✓		
Define scope of architecture	✓		
Determine depth of architecture	✓		
Select appropriate EA products			
Select products that represent business of enterprise	✓		
Select products that represent agency technical assets	✓		
Evaluate and select framework	✓		
Select EA toolset	✓		
Develop baseline enterprise architecture			
Collect information that describes existing enterprise		VA is validating its baseline application inventory; it is in the process of • developing detailed application profiles, • performing dynamic inventory modeling of baseline infrastructure, and • developing hardware and software profile information at server level	Complete baseline application inventory validation Complete detailed application profiles Complete baseline infrastructure inventory modeling Complete development of hardware and software profile information at server level Ensure that inventory includes all business functions and information flows, data models, external interface descriptions, and technical designs, specifications, and equipment inventories

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	Examples of key actions yet to be performed
Generate products and populate EA repository			Create and populate the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models			Have subject matter experts assess the enterprise architecture products for accuracy and completeness
Develop target enterprise architecture			
Collect information that defines future business operations and supporting technology: •strategic business objectives •information needed to support business •applications to provide information •technology to support applications		VA is collecting information and adding it to the Zachman framework to define the to-be architecture for telecommunications	Collect proposed business processes and information flows, strategic plans, modernization plans, and requirements documents; incorporate technology forecast, standards profile, and technical reference model
Generate products and populate EA repository			Create and populate the EA repository with products that describe the relationships among information elements and work products
Review, validate, and refine models			Have subject matter experts assess the enterprise architecture products for accuracy and completeness
Develop sequencing plan			Address all detailed activities in this step
Identify gaps			
Define and differentiate legacy, migration, and new systems			
Plan migration			
Approve, publish, and disseminate EA products			
Use enterprise architecture			Address all detailed activities in this step
Integrate EA with capital planning and investment control and systems life cycle processes			
Train personnel			
Establish enforcement processes and procedures			
Define compliance criteria and consequences			
Set up integrated reviews			
Execute integrated process			
Initiate new and follow-up projects			
Prepare proposal			
Align project to EA			
Make investment decision			

Steps in the enterprise architecture (EA) process[a]	Steps VA has completed	Examples of actions VA has planned or taken	Examples of key actions yet to be performed
Execute projects			
Manage and perform project development			
Evolve EA with program/project			
Assess progress			
Complete project			
Deliver product			
Assess architecture			
Evaluate results			
Consider other uses of EA			
Maintain enterprise architecture			Address all detailed activities in this step
Maintain EA as enterprise evolves			
Reassess EA periodically			
Manage projects to reflect reality			
Ensure business direction and processes reflect operations			
Ensure current architecture reflects system evolution			
Evaluate legacy system maintenance requirements against sequencing plan			
Maintain sequencing plan as integrated program plan			
Continue to consider proposals for EA modifications			

[a]Chief Information Officer Council.
[b]A repository is an information system used to store and access architectural information, relationships among the information elements, and work products.

Source: GAO analysis.

Among the key activities requiring immediate attention is establishment of a program management office headed by a permanent chief architect to manage the development and maintenance of the enterprise architecture. VA has begun establishing such an office and is currently recruiting a chief architect. However, until the department has an office that is fully staffed with experienced architects and hires a chief architect with the requisite core competencies, it will continue to lack the management and oversight necessary to ensure the success of its enterprise architecture program. Further, until the department has completed an implementation plan that delineates how it will develop, use, and maintain the enterprise architecture, it will lack definitive guidance for effectively managing the enterprise architecture program.

Further, a lot of work lies ahead related to VA's efforts toward developing its baseline and target architectures. A crucial first step in building the enterprise architecture is identifying and collecting existing products that

describe the agency as it exists today and as it is intended to look and operate in the future. While VA has developed a baseline application inventory to describe its "as is" state, it has not yet completed validating the inventory, or completed detailed application profiles for the inventory, including essential information such as business functions, information flows, and external interface descriptions. Similarly, to define its vision of future business operations and supporting technology, VA must still collect crucial information for its target architecture, including information on its proposed business processes, strategic plans, and requirements.

Beyond these planning and development activities, VA will also have to ensure the successful transition and implementation of its enterprise architecture. Evolving the agency from its baseline to the target architecture will require concurrent, interdependent activities and incremental development. As such, VA will need to develop and maintain a sequencing plan to provide a step-by-step approach for moving from the baseline to the target architecture. Development of this sequencing plan should consider a variety of factors, including sustaining of operations during the transition, anticipated management and organizational changes, and business goals and operational priorities. Ultimately, VA's success in using the architecture will depend on active management and receptive project personnel, along with effective integration of the enterprise architecture process with other enterprise life cycle processes.

A key aspect of VA's enterprise architecture program is the integration of security practices into the enterprise architecture. The CIO Council has articulated guidelines for doing so.[6] For example, the architecture policy should include security practices and the architecture team should include security experts. In its enterprise architecture strategy document, VA has committed to including security in all elements of its enterprise architecture. Further, VA's executive-level security officer served as a member of its architecture team. As VA moves forward in developing, implementing, and using its enterprise architecture, we would expect it to include information security details relating to the design, operations, encryption, vulnerability, access, and use of authentication processes. A commitment to building information security into all elements of its enterprise architecture program is essential to helping VA meet the challenges that it faces in protecting its information systems and sensitive data.

As VA moves forward with its enterprise architecture management program, it should ensure that remaining critical process steps outlined in the federal CIO guidance are sufficiently addressed and completed within reasonable timeframes. With the enhanced management capabilities

[6]Chief Information Officer Council, *A Practical Guide to Federal Enterprise Architecture,* Version 1.0 (Washington, D.C., February 2001).

provided by an enterprise architecture framework, VA should be able to (1) better focus on the strategic use of emerging technologies to manage its information, (2) achieve economies of scale by providing mechanisms for sharing services across the department, and (3) expedite the integration of legacy, migration, and new systems.

Information Security Challenges Continue to Require Top Management Attention

Information security continues to be among the top challenges that the department must contend with. As you know, in carrying out its mission, VA relies on a vast array of computer systems and telecommunications networks to support its operations and store the sensitive information that it collects related to veterans' health care and benefits. VA's networks are highly interconnected, its systems support many users, and the department is increasingly moving to more interactive, Web-based services to better meet the needs of veterans. Effectively securing these computer systems and networks is critical to the department's ability to safeguard its assets, maintain the confidentiality of sensitive veterans' health and disability benefits information, and ensure the reliability of its financial data.

Mr. Chairman, when we last testified, VA had just established a department-level information security management program and hired an executive-level official to head it.[7] VA had also finalized an information security management plan to provide a framework for addressing longstanding departmentwide computer security weaknesses. However, as our testimony noted, the department had not implemented key components of a comprehensive, integrated security management program that are essential to managing risks to business operations that rely on its automated and highly interconnected systems. This condition existed despite our previous recommendation that VA effectively implement and oversee its computer security management program through assessing risks, implementing policies and controls, promoting awareness, and evaluating the effectiveness of information system controls at its facilities.[8] As with its enterprise architecture, the Secretary expressed his intent to implement measures that would remedy existing deficiencies in the department's security program.

The effects of not having a fully integrated computer security management program in place remain evident. Since the subcommittee's hearing on this topic last April, VA and its Office of Inspector General have continued to report pervasive computer security challenges. VA's September 2001 report on compliance with recently enacted government information

[7] GAO-01-550T.

[8] U.S. General Accounting Office, *VA Information Systems: Computer Security Weaknesses Persist at the Veterans Health Administration*, GAO/AIMD-00-232 (Washington, D.C.: September 8, 2000).

security reform legislation[9] revealed that the department had not implemented effective information security controls for many of its systems and major applications. Last October, VA's inspector general also reported that it had found significant problems related to the department's control and oversight of access to its systems, including that VA had (1) not adequately limited the access of authorized users or effectively managed user identifications and passwords, (2) not established effective controls to prevent individuals from gaining unauthorized access to its systems, (3) not provided adequate physical security to its computer facilities, and (4) not updated and tested disaster recovery plans to ensure continuity of operations in the event of a disruption in service.

Many of these access and other general control weaknesses mirror deficiencies we have reported since 1998, and that VA's inspector general continues to report as a material weakness in the department's internal controls.[10] Based largely on weaknesses of this type, last fall the House Government Reform Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations gave VA a failing grade in computer security.[11]

Progress Being Made, But Important Elements of a Comprehensive Computer Security Management Program Still Lacking

VA's senior leadership has shown greater awareness of and concern for the severity of the department's computer security problems, and since last April has taken steps aimed at strengthening VA's overall security posture. Specifically, to provide greater management accountability for information security, the secretary has mandated information security performance standards for members of the department's senior executive service. In addition, VA's cyber security officer—the department's senior security official—has organized his office to focus more directly on the

[9]The government information security reform provisions of the fiscal year 2001 Defense Authorization Act (P.L. 106-398) require annual agency program reviews and annual independent evaluations for both non-national security and national security information systems.

[10]Department of Veterans Affairs Office of Inspector General, *Report of the Audit of the Department of Veterans Affairs Consolidated Financial Statements for Fiscal Years 2001 and 2002* (Washington, D.C., February 27, 2002).

[11]House Committee on Government Reform. Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, *Computer Security: How Is the Government Doing?* 107th Cong., 1st sess., 9 November 2001.

critical elements of information systems control that are defined in our information system controls audit methodology.[12] Further, the department has adopted the National Institute of Standards and Technology's federal information technology security assessment framework to use in determining the current status of these controls and measuring the progress of information security program improvements.

The cyber security officer also recently revised the department's security management plan to update security policies, procedures, and technical standards. The updated plan outlines actions for developing risk-based security assessments, improving the monitoring and testing of systems controls, and implementing departmentwide virus-detection software and intrusion-detection systems. The plan places increased emphasis on centralizing key security functions that previously were decentralized or nonexistent, including virus detection, systems certification and accreditation, network management, configuration management, and incident and audit analysis.

Yet even with this positive direction, VA's actions do not fully address remaining problems, and are inadequate to cover the breadth of matters essential to a comprehensive security management program. Our 1998 report on effective security management practices used by several leading public and private organizations[13] and a companion report on risk-based security approaches in 1999[14] identified key principles that can be used to establish a management framework for more effective information security programs. This framework is depicted in figure 2. The leading organizations we examined applied these principles to ensure that information security addressed risks on an ongoing basis. Further, these have been cited as useful guidelines for agencies by the Federal CIO Council and incorporated into the council's information security assessment framework,[15] intended for agency self-assessments.

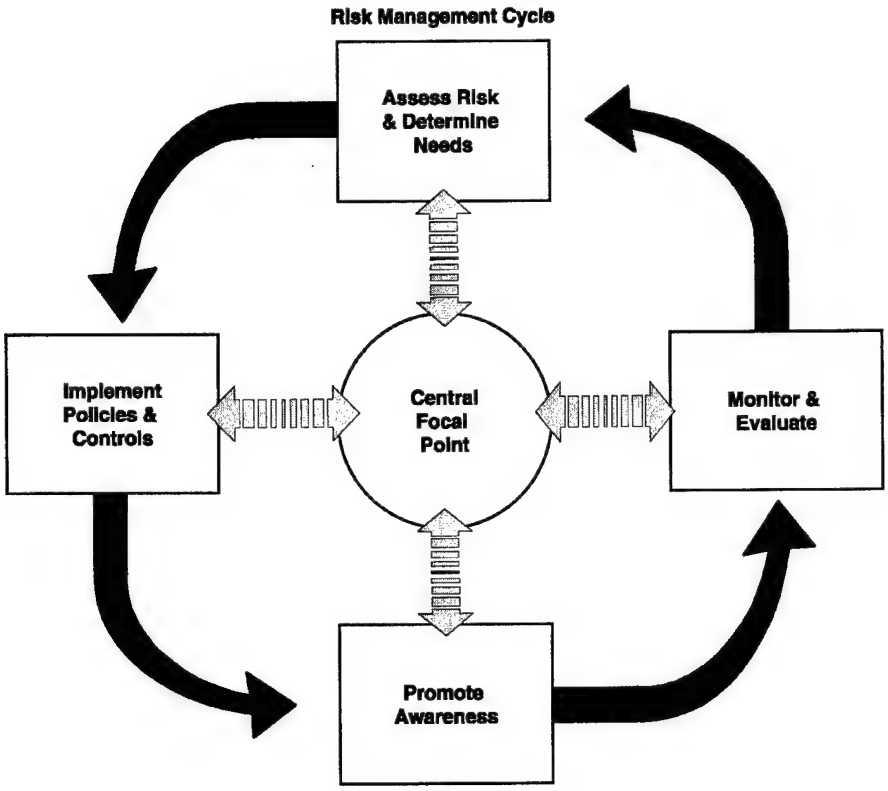
[12]U.S. General Accounting Office, *Federal Information System Controls Audit Manual,* GAO/AIMD-12.19.6 (Washington, D.C., January 1999).

[13]U.S. General Accounting Office, *Information Security Management: Learning From Leading Organizations,* GAO/AIMD-98-68 (Washington, D.C., May 1998).

[14]U. S. General Accounting Office, *Information Security Risk Assessment: Practices of Leading Organizations,* GAO/AIMD-00-33 (Washington, D. C., November 1999).

[15]Chief Information Officer Council, *Federal Information Technology Security Assessment Framework* (Washington, D.C., November 28, 2000).

Figure 2: Information Security Risk Management Framework



Source: GAO/AIMD-98-68.

Using our information security risk management framework as criteria, table 2 summarizes both the actions that VA has taken and those still needed to ensure that it has a comprehensive computer security management program. As shown, while VA has completed a number of important steps, its efforts in each of the five key areas of effective computer security program management—central security management, security policies and procedures, risk-based assessments, security awareness, and monitoring and evaluation—have not yet included key actions that are essential for successful and effective program implementation.

Table 2: Actions Needed to Ensure a Comprehensive Computer Security Management Program

Important elements of a computer security management program[c]	Actions VA has taken	Actions still needed
Central security management function to guide and oversee compliance with established policies and procedures and review effectiveness of the security environment	Established a department-level information security officer Began requiring full-time security officers or staff with primary duty for security at all facilities Established a CIO subcommittee to improve departmentwide coordination on security issues	Ensure full-time security officers or staff with primary duty for security are assigned to information security officer positions, and clearly define their roles and responsibilities Develop guidance to ensure authority and independence for security officers Develop policies and procedures to ensure departmentwide coordination of security functions
Security policies and procedures that govern a complete computer security program and integrate all security aspects of an organization's environment, including local area networks, wide area networks, and mainframe security	Updating department security policy and guidance Developed technical security standards for some network platforms	Refocus department policy to address security from an interconnected VA systems environment perspective in addition to that of individual systems Develop and implement technical security standards for mainframe and other systems and security software
Periodic risk assessments to assist management in making decisions on necessary controls to help ensure that security resources are effectively distributed to minimize potential loss	Developed abbreviated risk methodology as part of the Government Information Security Reform Act process Established policy requiring risk to be assessed when significant changes are made to computer systems	Include best minimum standards or guidance for performing risk assessments in methodology Develop guidance for determining when an event is a significant change and explaining the level of risk assessment required for these system changes

Important elements of a computer security management program[c]	Actions VA has taken	Actions still needed
Security awareness to educate users about current information security risks, policies, and procedures	Implemented a departmentwide security awareness program	Establish a process to ensure program compliance
Monitoring and evaluating computer controls to ensure their effectiveness, improve them, and oversee compliance	Issued contract for independent compliance reviews of ongoing initiatives related to security controls Performed penetration testing of its Web sites from the Internet Implemented computer virus-detection software departmentwide Began developing an inventory of security weaknesses Established a process for reporting computer security incidents and piloted intrusion-detection systems at selected locations Developed a certification and accreditation framework for its general support and major applications	Develop specific requirements for conducting compliance review program Develop an ongoing program for testing controls to include assessments of both internal and external access to VA systems; expand current tests to identify unauthorized or vulnerable external connections to VA's network Establish a process for tracking the status of security weaknesses, corrective actions taken, and independent validation of the corrective actions Develop a process for routinely analyzing the results of computer security reviews to identify trends and vulnerabilities and apply appropriate countermeasures to improve security Develop a proactive security incident response program to monitor user access for unusual or suspicious activity

[c]U.S. General Accounting Office, *Executive Guide: Information Security Management*, GAO/AIMD-98-68 (Washington, D.C.: April 7, 1998).

Source: GAO analysis.

As the table illustrates, VA's security management program continues to lack essential elements required to protect the department's computer systems and networks from unnecessary exposure to vulnerabilities and risks. For example, while VA has begun to develop an inventory of known security weaknesses, it continues to be without a comprehensive, centrally managed process that will enable it to identify, track, and analyze all computer security weaknesses. Further, the updated security management plan does not articulate critical actions that VA will need to take to correct specific control weaknesses or the time frames for completing key actions. While the plan calls for monitoring VA's computer control environment to ensure compliance, the plan does not provide a framework to guide the monitoring activities by, for example, identifying the specific security areas to be reviewed, the scope of compliance work to be performed, the frequency of reviews, reporting requirements, or the resolution of reported issues.

VA also lacks a mechanism for collecting and tracking performance data, ensuring management action as needed and, when appropriate, providing independent validation of program deliverables. Without these essential

elements, VA will have only limited assurance that its financial information and sensitive medical records are adequately protected from unauthorized disclosure, misuse, or destruction. Accordingly, as VA continues to improve upon its information security management, it should move expeditiously to address the gaps we are highlighting in table 2.

In commenting on the department's current security posture, VA's cyber security officer stated that efforts are planned or underway to address the actions not yet completed. He added that by August 31, 2002, the department expects to have a plan for completing all of the necessary corrective actions.

Overarching Organizational and Management Issues Could Hinder VA's Ability to Fully Address Information Security Challenges

While VA is clearly placing greater emphasis on its information security, its cyber security officer will be challenged to manage the security function on a departmentwide basis. As the department is currently organized, more than 600 information security officers in VA's three administrations and its many medical facilities throughout the country[16] are responsible for ensuring that appropriate security measures are in place. These information security officers report to their facility's director or the chief information officer for their administration. However, there is neither direct nor indirect reporting to VA's cyber security officer, thus raising questions about this official's ability to enforce compliance with security policies and procedures and ensure accountability for actions taken throughout the department. Further, because VA's information security budget relies on funding by its component administrations, the cyber security officer lacks control and accountability over a significant portion of the financial resources that the security program depends on to sustain its operations.[17]

Successfully managing information security under this organizational structure, therefore, will in large part depend on the extent to which VA's business managers assume responsibility for implementing the appropriate policies and controls to mitigate risks, and work collaboratively and cooperatively with the cyber-security officer. Consequently, it will be essential for VA to hold its senior managers accountable for information security at their respective facilities and administrations. VA has taken a critical step toward achieving this by establishing security performance standards for its senior executives. These standards must be effectively applied and enforced, however, to ensure a successful outcome.

[16]VHA provides medical care at 163 hospitals, more than 800 community and facility-based clinics, 135 nursing homes, 43 domiciliaries, 206 readjustment counseling centers, and various other facilities.

[17]For example, to help support its fiscal year 2002 security program budget request of about $55 million, VA expects to receive about $22 million in funding from VHA and $12 million from the department's other administrations and offices.

Progress on the Compensation and Pension Replacement System Is Disappointing

The VETSNET compensation and pension replacement effort grew out of an initiative that VBA undertook in 1986 to replace its outdated benefits delivery network (BDN) and modernize its compensation and pension, education, and vocational rehabilitation benefits payment systems. VBA had expected these modernized systems to provide a rich source for answering questions about veterans' benefits and enable faster processing of benefits. In 1996, after experiencing numerous false starts and spending approximately $300 million on the overall modernization, VBA revised its strategy and began focusing on modernizing the compensation and pension (C&P) payment system. At that time, VBA estimated that the C&P replacement project would cost $8 million and be completed in May 1998.

Since its inception, however, VBA has been plagued with problems in carrying out the C&P replacement initiative. As detailed in the attachment, our various publications since 1996 have highlighted consistent and longstanding concerns in several areas, including project management, requirements development, and testing. Our testimony last April noted that VBA had made some progress in developing and testing software products that would become part of the system. Nevertheless, we also noted that VBA had not addressed several important issues that were key to its successful implementation, including the need to develop an integrated project plan and schedule incorporating all of the critical areas of this system development effort.[18] As our prior work has pointed out, a significant factor contributing to VBA's continuing problems in developing and implementing the system has been the level of its capability to develop and maintain high-quality software on any major project within existing cost and schedule constraints—a condition that we identified during our 1996 assessment of the department's software development capability.[19]

Critical Actions Have Not Been Taken to Ensure Successful Implementation of the C&P Replacement System

After 6 years of work—4 years beyond what its initial estimate called for—VBA has spent at least $35 million, without much demonstrable progress toward implementing the replacement system. Since last April, it has not made substantial progress in addressing the concerns raised by our earlier work. Although, last year, VBA indicated that it had implemented its rating board automation tool and had completed developing and testing its four other software products,[20] the administration stated during our recent review that two of the software products that will support its award processing and finance and accounting systems still need further

[18]GAO-01-550T.

[19]U.S. General Accounting Office, *Software Capability Evaluation: VA's Software Development Process is Immature*, GAO/AIMD-96-90 (Washington, D.C.: June 19, 1996).

[20]The current C&P replacement strategy incorporates five software products: Search and Participant Profile, Rating Board Automation 2000, Modern Award Processing-Development, Award Processing, and Finance and Accounting System. The first product deployed in November 2000—Rating Board Automation 2000—was to assist veterans service representatives in rating benefits claims.

development. Moreover, VBA has not increased the number of payments using these new software products beyond the 10 original claims that it had pilot tested in February 2001. In addition, it continues to lack an integrated project plan and schedule that incorporate all of the critical areas of this system development activity. Further, VBA still has not obtained essential support from the field office staff that will be required to use the new software, and requirements for the new software have not yet been validated. These deficiencies are significant, given that the software application that VBA developed to assist veterans service representatives in rating benefits claims (Rating Board Automation 2000) did not meet users' needs and achieved less timely claims processing results.

At this time, VBA also is without a project manager to oversee the project. Progress made early in 2000 toward creating a project control board to manage the C&P replacement was curtailed when the project manager departed last April. Until VBA provides appropriate management and oversight for all aspects of the project's development and implementation, it will not be positioned to ensure that this project will deliver a cost-effective solution with measurable and specific program-related benefits.

Further, the schedule for implementing the replacement system continues to undergo change, resulting in additional delays. Last April, VBA had planned to deploy VETSNET in all of its 58 regional offices in July 2002. However, VBA officials have since modified the deployment time frame twice, with its latest proposal being to deploy each of the five applications separately over 2 years, beginning in June 2003. VBA management has not yet approved this latest strategy.

Studies Highlight the Need for Additional Testing and Information to Support Continued Systems Development

Last year, the secretary expressed concerns about the VETSNET project and called for an independent audit of the C&P replacement system to facilitate his decision on whether to continue the initiative. Accordingly, a contractor was hired in May 2001 to assess (1) whether the system architecture will be capable of supporting VBA's projected future workload, and (2) whether the system being developed will meet future functional, performance, and security needs. The contractor reported last September that the system architecture would be able to process VBA's projected future workload.

However, the contractor neither assessed nor reported on whether the system will meet future functional business needs, and the scope of its review did not generate sufficient information to fully evaluate and make an informed decision on whether the project should proceed. The review focused primarily on the system's ability to perform efficiently under a heavy workload, and did not include user acceptance or the functional testing that is needed to ensure that the system can fully satisfy user requirements and that deployed software can be used without significant errors. Further, the review did not fully address the security requirements

for the new system. VA's department-level CIO agreed that the scope of the contractor's review had been limited to a technical review of whether VETSNET could handle the anticipated workload. He also acknowledged the need for functional testing and an integrated project plan.

Similar concerns about VBA's strategy for the C&P replacement project were also documented in an October 2001 report issued by the VA claims processing task force.[21] In its report, the task force emphasized that limited user and functional testing posed a major problem for VBA in developing and implementing its systems. The task force highlighted material deficiencies in VBA's strategic planning and its implementation and deployment of new and enhanced information technology products and initiatives, as had been pointed out in an earlier report. Further, the task force questioned whether VETSNET represented a viable long-term solution, in part because it does not provide support for a redesigned and integrated claims process across VA's administrations and offices.

In commenting on these reports' findings, VBA's CIO stated that, by the end of March 2002, her office anticipated completing a remediation plan that will address the most critical concerns identified in the contractor's review. She stated that the office is in the process of developing a statement of work to obtain contractor support to develop additional functional testing capability. The statement of work is scheduled for completion in June 2002. In addition, the CIO is negotiating with relevant VBA business groups to secure subject matter experts to validate business requirements and assist with the functional testing.

VETSNET Deployment Delays Affect the Benefits Delivery Network

If not promptly addressed, the problems and delays that have been noted in implementing the VETSNET project could have critical cost implications for the department and service delivery inefficiencies for the veteran community. In particular, without a replacement system, VA must continue to rely on the aging BDN to deliver its benefit payments, parts of which were developed in the 1960s. Although the BDN was enhanced to address year 2000 conversion issues, because of its anticipated replacement, VBA has since made only limited investments in maintaining it.

[21]The claims processing task force was formed in May 2001, when the secretary of veterans affairs asked a group of individuals with significant VA experience to assess and critique VBA's compensation and pension organization, management, and processes and to develop recommendations to significantly improve VBA's ability to process veteran claims for disability compensation and pension.

Without additional maintenance, it is uncertain that the BDN will be able to continue accurately processing the many benefits payments that VBA must make.[22] In its report, the claims processing task force warned that the system's operations and support were approaching a critical stage, with the potential for performance to degrade and eventually cease. The task force recommended that the BDN be sustained and upgraded to ensure that payments to veterans would remain prompt and uninterrupted until VBA is able to field a replacement system. VBA officials have stated that they are working on a plan to address this issue. This plan is expected to include purchasing an additional mainframe computer to help extend the system's operation until 2007—the date by which new systems are planned to be operational for all three benefits payment business lines.

As you can see, Mr. Chairman, despite many years of work, VBA still has a number of fundamental tasks to accomplish before it can successfully complete development and implementation of the VETSNET project. Before proceeding with this project, VBA must assess and validate users' requirements for the new system to ensure that business needs are met. It also needs to complete testing of the system's functional business capability, as well as end-to-end testing to ensure payments are made accurately. Finally, it must establish an integrated project plan to guide its transition from the old to the new system. Until VBA performs a complete analysis of the initiative, as the secretary has indicated he would do, it is questionable whether additional resources should be expended on continued systems development activities.

VHA Continues to Expand Its Use of DSS

Unlike VBA's work on VETSNET, VHA continues to make progress in expanding overall use of its decision support system (DSS). As you know, DSS is an executive information system designed to provide VHA managers and clinicians with data on patterns of patient care and patient health outcomes, as well as the capability to analyze resource utilization and the cost of providing health care services. VHA completed its implementation of DSS in October 1998. However, in September 2000, we testified that DSS had not been fully utilized since its implementation, and noted that DSS was not being used for all the purposes intended.[23]

Last April, we testified that VHA had shown moderate progress in increasing usage of DSS among its veterans integrated service networks (VISN) and medical centers, and encouraged VA to continue providing top management support to ensure that the system is fully utilized and that financial and clinical benefits are realized. Our testimony noted several

[22]The current C&P payment system alone processes about 3.2 million payments each month. Altogether, the three benefits payment business lines process about 3.5 million payments monthly.

[23] GAO/T-AIMD-00-321.

efforts that VHA had undertaken to encourage greater use of DSS, including using DSS data to support the fiscal year 2002 resource allocation process and as a consideration in preparing VISN directors' year-end performance appraisals, requiring VISN directors to provide examples of their reports and processes that rely on DSS data, and ensuring that medical centers' processing of DSS data is current (no more than 60 days old).[24]

VHA's initiatives to encourage greater use of DSS have yielded results. The use of DSS data in the fiscal year 2002 allocation process has clearly raised VHA's awareness about the importance of this information. VHA's most recent DSS processing report, dated January 31, 2002, revealed that all 22 VISNs had completed processing fiscal year 2001 DSS data and that seven VISNs had begun processing fiscal year 2002 data. Further, every VISN has provided both clinical and financial examples of DSS usage, and this information is now being considered in the quarterly reviews of the VISN directors' performance. As a result, VHA's managers have grown more knowledgeable about and have begun to make more informed decisions regarding the cost of care being provided by their facilities.

Initiatives Are Being Taken to Improve the Accuracy, Timeliness, and Availability of DSS Data

VHA continues to explore other initiatives to improve the accuracy and completeness of DSS data. In response to a report issued by VA's inspector general in March 1999,[25] regarding the failure of some medical facilities to follow the DSS basic structure for capturing workload data and associated costs, VHA has taken several actions, including

- implementing a VHA decision support system standardization directive that requires annual standardization audits and the reporting of consecutive repeat occurrences of non-compliance to the assistant deputy under secretary for health;
- developing an audit tool for use in determining a facility's compliance with the DSS basic model for capturing workload data and associated costs; and
- performing a standardization audit in September 2001 to assess the extent to which each facility's DSS departments and products complied with national standards.[26]

[24]GAO-01-550T.

[25]Department of Veterans Affairs, Office of Inspector General, *Audit of Veterans Health Administration Decision Support System Standardization*, Report No. 9R4-A19-075 (Washington, D.C., March 31, 1999).

[26]The standardization audit revealed a 99.6 percent compliance rate with the National Department List, a 98.8 percent compliance rate with the National Product List, and a 99.5 percent match between facilities' cost centers and DSS departments.

Further, in response to managers' concerns that DSS data are not timely and easy to access, the DSS program office initiated several actions. These include establishing a working group last July to identify best practices and recommend actions for improving processing efficiency and the timeliness and availability of DSS data. To date, the working group has provided all DSS sites with an updated monthly guide detailing each step of the process, and has distributed a pharmacy rejects database and a step-by-step guide for processing these rejects. These products should help increase the efficiency of the monthly processing and facilitate more accurate and timely data. In addition, the program office has authorized two sites to pilot test an application aimed at providing the end user or manager with a user-friendly front end to display DSS information and allow patient inquiry.

In addition, several VISNs have independently begun exploring options for providing easier access to DSS data. For example, one is examining the feasibility of establishing a data warehouse where data extracted from DSS can be transformed into a format that will facilitate queries and reports that are simple to create and quick to run.[27] Another has begun building a data repository for use in creating an application to compile and deliver data requested by managers or clinicians.[28]

Even with these accomplishments, however, top management involvement and continued support will be critical to ensuring that VHA continues to make progress in improving the operational efficiency and effectiveness of DSS, and that it realizes the full clinical and financial benefits of this system. In March 2001, oversight for the DSS program was transferred from VHA's chief information officer to its chief financial officer. Since that time, VHA has also assigned three different acting directors to lead the program. However, VHA has not yet selected a permanent director to provide consistent management and oversight. In addition, of 56 personnel positions allotted to the DSS program office, 19 positions had not been filled at the end of January 2002. Without a permanent director to lead the DSS program or full staffing to support the system's operation, VHA runs the risk that continued increases in usage of DSS, along with its associated benefits, could be imperiled.

[27] Veterans integrated service network 16 (Jackson, Mississippi).

[28] Veterans integrated service network 13 (Minneapolis, Minnesota)

The Government Computer-based Patient Record Initiative Is Moving Away From Its Original Goal

Mr. Chairman, you also asked us to update you on VA's progress, in conjunction with the Department of Defense (DOD) and the Indian Health Service (IHS), in achieving the ability to share patient health care data as part of the government computer-based patient record (GCPR) project. Having readily accessible data to facilitate services to our nations' military personnel and others has proved particularly significant in light of recent terrorist actions and the associated responses that have been required.

The GCPR project developed out of VA and DOD discussions about ways to share data in their health information systems and from efforts to create electronic records for active duty personnel and veterans. As you know, the patients served by VA's and DOD's systems tend to be highly mobile, and consequently, their health records may be at multiple federal and nonfederal medical facilities, both in and outside of the United States. In November 1997, the president called for the two departments to develop a "comprehensive, life-long medical record for each service member," and in August 1998—8 months after the GCPR project was officially established—issued a directive requiring VA and DOD to develop a "computer-based patient record system that will accurately and efficiently exchange information."[29] IHS later became involved because of its expertise in population-based research and its longstanding relationship with VA in caring for the Indian veteran population.

As originally envisioned, GCPR was not intended to be a separate computerized health information system, nor was it meant to replace VA's, DOD's, and IHS's existing systems. Rather, it was intended to allow physicians and other authorized users at these agencies' health facilities to access data from any of the other agencies' health facilities by serving as an electronic interface among their health information systems. The interface was expected to compile requested patient information in a temporary, "virtual" record, that could be displayed on a user's computer screen.

In April 2001, we reported that expanding time frames and cost estimates, as well as inadequate accountability and poor planning, tracking and oversight, had raised doubts about GCPR's ability to provide the benefits expected.[30] In particular, we noted that the project's time frames had significantly expanded and that its costs had continued to increase. In

[29]National Science and Technology Council, *A National Obligation: Planning for Health Preparedness for and Readjustment of the Military, Veterans, and Their Families After Future Deployments,* Presidential Review Directive 5 (Washington, D.C., Executive Office of the President, Office of Science and Technology Policy, August 1998).

[30]U. S. General Accounting Office, *Computer-Based Patient Records: Better Planning and Oversight by VA, DOD, and IHS Would Enhance Health Data Sharing,* GAO-01-459 (Washington, D.C., April 30, 2001).

addition, basic principles of sound IT project planning, development, and oversight had not been followed, creating barriers to progress. For example, clear goals and objectives had not been set; detailed plans for developing, testing, and implementing the new software had not been established; and critical decisions regarding goals, costs, and time frames were not binding on all parties. Further, data exchange and privacy and security issues critical to the project's success remained to be addressed.

As a result of these concerns, we recommended that the three agencies (1) designate a lead entity with final decisionmaking authority and establish a clear line of authority for the GCPR project and (2) create comprehensive and coordinated plans that included an agreed-upon mission and clear goals, objectives, and performance measures, to ensure that the agencies can share comprehensive, meaningful, accurate, and secure patient health care data. In commenting on the report, VA, DOD, and IHS all concurred with our findings and recommendations.

Nonetheless, progress on the GCPR initiative continues to be disappointing. The scope of the project increasingly has been narrowed from its original objectives and it continues to proceed without a comprehensive strategy. For example, in responding to our report, VA, DOD, and IHS provided information on a new, near-term strategy for GCPR. However, this revised strategy is considerably less encompassing than the project was originally intended to be. Specifically, rather than serve as an interface to allow data sharing across the three agencies' disparate systems, as originally envisioned, a first phase of the revised strategy calls only for a one-way transfer of data from DOD's current health care information system to a separate database that VA hospitals can access. While even this degree of data sharing is a positive development, VA's clinicians, nonetheless, will only be allowed to read, but not perform any calculations on the data received. VA and DOD officials had initially planned to implement this near-term capability in November 2001, but recently stated that they now expect to do so by this July 2002. Further, the officials stated that they plan to change the name of the project to the Federal Health Information Exchange.

Subsequent phases of the effort that were to further expand GCPR's capabilities have also been revised. A second phase that would have enabled information exchange among all three agencies—VA, DOD, and IHS—is now expected to enable only a bilateral read-only exchange of data between VA and IHS.

Further, according to VA officials, plans for a third phase, which was to expand GCPR's capabilities to public and private national health information standards groups, are no longer being considered for the project. Instead, the third phase is now expected to focus only on expanding the data exchange between VA and IHS and allowing limited data calculations and some translation of terminology between the two

agencies. Under the revised strategy, there are no plans for DOD to receive data from VA.

In addition, concerns expressed in our April 2001 report still need to be addressed. For example, the GCPR project continues to operate without clear lines of authority or a lead entity responsible for final decisionmaking. Last August, the VHA CIO informed us that a draft memorandum of agreement, designating VHA as the lead entity, was being considered within VA, DOD, and IHS. However, this memorandum had not been approved or implemented at the time that we concluded our review. The project also continues to move forward without comprehensive and coordinated plans, including an agreed-upon mission and clear goals, objectives, and performance measures. Without clearly defined lines of authority and a comprehensive and coordinated strategy, even the revised GCPR initiative is destined to continue on an uncertain course—one that is unlikely to deliver substantial results.

* * * * *

In summary, VA has made good progress toward addressing a number of important information technology concerns, but it still has much work to do. Its current leadership is to be commended for the dedication that it has demonstrated regarding VA's information technology problems. However, in totality, the steps taken to date have not been sufficient to overcome the wide range of deficiencies that threaten VA's operational effectiveness. Many of VA's problems are longstanding and pervasive, and can be attributed to fundamental weaknesses in management accountability—some of which can only be overcome through serious restructuring of current reporting relationships and lines of authority. Until VA makes a concerted effort to ensure that all necessary processes and controls exist to guide the management of its information technology program, it will continue to fall short of its goals of enhancing operational efficiency and, ultimately, improving service delivery to our nation's veterans.

Mr. Chairman, this concludes my statement. I would be pleased to respond to any questions that you or other members of the subcommittee may have at this time.

Contacts and Acknowledgments

For information about this testimony, please contact me at (202) 512-6257 or by e-mail at mcclured@gao.gov. Individuals making key contributions to this testimony included Nabajyoti Barkakati, Amanda C. Gill, David W. Irvin, Tonia L. Johnson, Valerie C. Melvin, Barbara S. Oliver, J. Michael Resser, Rosanna Villa, and Charles M. Vrabel.

GAO Products Highlighting Concerns with VETSNET C&P Replacement

Issuance date Report/testimony	Summary of report findings and conclusions
April 4, 2001 GAO-01-550T	The project's viability was still a concern. It continued to lack an integrated project plan and schedule addressing all critical systems development areas, to be used as a means of determining what needs to be done and when. A pilot test of 10 original claims that did not require significant development work may not have been sufficient to demonstrate that the product was capable of working as intended in an organizationwide operational setting.
September 21, 2000 GAO/T-AIMD-00-321	VBA's software development capability remained ad hoc and chaotic. The VETSNET implementation approach lacked key elements, including a strategy for data conversion and an integrated project plan and schedule incorporating all critical systems development areas. Further, data exchange issues had not been fully addressed.
May 11, 2000 GAO/T-AIMD-00-74	$11 million had reportedly been spent on VETSNET C&P; both the May 1998 completion date and revised completion date of December 1998 were not met. Contributing factors included lack of an integrated architecture defining the business processes, information flows and relationships, business requirements, and data descriptions, and VBA's immature software development capability.
September 15, 1997 GAO/AIMD-97-154	VBA's software development capability remained ad hoc and chaotic, subjecting the agency to continuing risk of cost overruns, poor quality software, and schedule delays in software development.
May 30, 1997 GAO/AIMD-97-79	VETSNET experienced schedule delays and missed deadlines because (1) it employed a new software development language not previously used by the development team, one that was inconsistent with the agency's other systems development efforts; (2) the department's software development capability was immature and it had lost critical systems control and quality assurance personnel, and (3) VBA lacked a complete systems architecture; for example, neither a security architecture nor performance characteristics had been defined for the project.
June 19, 1996 GAO/T-AIMD-96-103	VETSNET had inherent risks in that (1) it did not follow sound systems development practices, such as validation and verification of systems requirements; (2) it employed a new systems development methodology and software development language not previously used; and (3) VBA did not develop the cost-benefit information necessary to track progress or assess return on investment (for example, total software to be developed and cost estimates).
June 19, 1996 GAO/AIMD-96-90	VBA's software development capability was immature and it could not reliably develop and maintain high-quality software on any major project within existing cost and schedule constraints, placing its software development projects at significant risk. VBA showed significant weaknesses in requirements management, software project planning, and software subcontract management, with no identifiable strengths.

(310419)